

Project	IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>	
Title	Correction to TFTP-RSP message	
Date Submitted	2004-04-28	
Source(s)	Itzik Kitroser Yossi Segal Yigal Leiba Zion Hadad Runcom Technologies Ltd. 2 Hachoma St. 75655 Rishon Lezion, Israel	Voice: +972-3-9528440 Fax: +972-3-9528805 mailto:itzikk@runcom.co.il mailto:yossis@runcom.co.il mailto:yigall@runcom.co.il mailto:zionh@runcom.co.il
Re:	802.16-REVd Sponsor ballot recirc	
Abstract	This contribution provides correction to an undefined state or authentication failure in the TFTP-CPLT message	
Purpose	Adopt suggested changes into P802.16-REVd/D4 draft	
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.	
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.	
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures < http://ieee802.org/16/ipr/patents/policy.html >, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair < mailto:chair@wirelessman.org > as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site < http://ieee802.org/16/ipr/patents/notices >.	

Correction to TFTP-RSP message

Itzik Kitroser

Yossi Segal

Yigal Leiba

Zion Hadad

Runcom Technologies Ltd.

General

In the TFTP-CPLT message, the SS must send HMAC tuple for authentication, while in the TFTP-RSP there is no response field. This means that the case of authentication failure the state is undefined. If the SS does not receive an answer, then it doesn't know if it because of authentication failure or the messages was lost, and will have to time-out and retransmit.

Editorial instruction is indicated by a **red bold** text with square brackets. Deletions are indicated by a ~~strikethrough~~ text and new text insertion is indicated by an underline.

Proposed changes

[Page 77, line 49, section 6.3.2.3.29 change as indicated]

6.3.2.3.29 Config File TFTP Complete Response (TFTP-RSP) message

The Config File TFTP-RSP message shall be generated by the BS in response to a TFTP-CPLT message from the SS (see 6.3.9.12). The format of the TFTP-RSP shall be as shown in Table 1.

Table 1—Config File TFTP-RSP message format

Syntax	Size	Notes
TFTP-RSP_Message_Format() {		
Management Message Type = 32	8 bits	
<u>Response</u>	<u>8 bits</u>	
}		

Parameters shall be as follows:

CID (*in the generic MAC header*)
SS's Primary Management CID.

Response

A 1 byte quantity with one of the two values:
0 = OK
1 = Message authentication failure

[Page 168, line 53, section 6.3.9.12 change paragraph as indicated]

When the configuration file download has completed successfully, the SS shall notify the BS by transmitting a TFTP-CPLT message on the SS's primary management connection. Transmissions shall continue periodically until a TFTP-RSP message is received with OK response from the BS (see Figure 69 and Figure 70) or the SS terminates retransmission due to retry exhaustion.

[Page 170, line 29, section 6.3.9.12 change figure 69 as indicated]

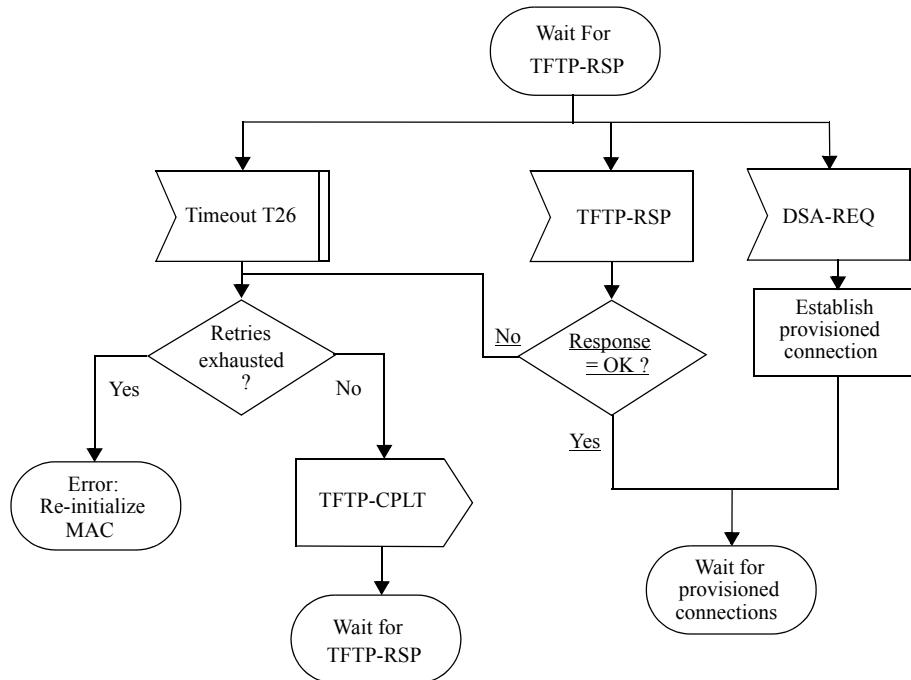


Figure 69—Wait for TFTP-RSP—SS

[Page 170, line 29, section 6.3.9.12 switch between figure 69 and figure 70]